Cryptographic Hash Workshop
NIST Gaithersburg, MD (Green Auditorium)
Oct. 31-Nov. 1, 2005
Submission deadline: July 15, 2005 (Workshop without proceedings)

Recently a team of researchers reported that the SHA-1 function offers significantly less collision resistance than could be expected from a cryptographic hash function of its output size. NIST plans to host a Cryptographic Hash Workshop on Oct. 31-Nov. 1, 2005 to solicit public input in how best to respond to the current state of research in this area. The workshop has the following goals:

- Assess the status of the current NIST-approved hash functions, i.e., the SHA-256 and SHA-512 families in addition to SHA-1;
- Discuss short term actions to mitigate the potential problems with the various applications of the approved hash functions;
- Discuss the conditions that would warrant an early transition away from any of the approved hash functions;
- Discuss the potential replacement options for any of the approved hash functions;
- Clarify the properties of unkeyed cryptographic hash functions required for different applications.

NIST solicits papers, presentations, case studies, panel proposals, and participation from any interested parties, including researchers, systems architects, vendors, and users. NIST will post the accepted papers and presentations on the workshop web site and include these in a workshop handout. However, no formal workshop proceedings will be published. NIST encourages presentations and reports on preliminary work that participants plan to publish elsewhere. Topics for submissions should include, but are not limited to, the following:

Security Status of Approved Hashes
- The latest results on the security of SHA-1;
- The latest results on the security of the SHA-256 and SHA-512 families of hash functions;
- Likely extensions to the latest results on the approved hash functions;
- The impacts of the latest results on different applications of the approved hash functions.

Short Term Actions
- How urgent are the current concerns with the approved hash functions?
- What changes to applications and protocols could mitigate potential problems?
- What guidance should NIST give with respect to hash functions and their applications?

Conditions for an Early Transition
- How can hash functions be assessed for security properties such as collision resistance, preimage resistance, and pseudo-randomness?
- What conditions would warrant a transition away from one of the approved hashes that is earlier than currently planned?

Potential Replacement Options
- Hash functions currently available for replacing one of the approved hash functions;
- What paradigms other than the Merkle-Damgård construction might be appropriate to consider?

- The need for an open competition, along the lines of the AES competition, for designing a new hash function.

Requirements for Unkeyed Cryptographic Hash Functions

- Desirable (or undesirable) general properties of hash functions for security, performance, and implementability;
- Desirable (or undesirable) properties of hash functions for particular applications, such as digital signatures, key derivation, message authentication, and random number generation;
- Identifying and encouraging the proper use of hash functions for particular applications.

Deadlines for submissions are:

- **Papers, Presentations, and Proposals Due: July 15, 2005**
- **Authors Notified: August 31, 2005**

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). Paper submissions must not exceed 15 pages (single space, two column format with 1" margins using a 10 pt or larger font) and have no header or footer text (e.g., no page numbers). Proposals for presentations or panels should be no longer than five pages; panel proposals should include possible panelists and an indication of which panelists have confirmed participation.

Please submit the following information to **hash-function@nist.gov**

- Name, affiliation, email, phone, postal address for the primary contact author
- First name, last name, and affiliation of each co-author
- The finished paper, presentation, or panel proposal in PDF format as an attachment.

All submissions will be acknowledged.

General information about the workshop including the registration and accommodation information is available at the workshop website: http://www.nist.gov/hash-function